2012

Servidor SSH

Manual de usuario SSH

Inicialmente la administración remota se hacía con la orden Telnet. En la actualidad no se debería utilizar Telnet por los importantes agujeros de seguridad que presenta. La transmisión entre cliente y el servidor se realiza completamente en texto plano (sin cifrar), por lo que con cualquier sniffer es posible capturar tramas y obtener de ellas login y la contraseña del usuario. En la actualidad la herramienta de administración remota más utilizada es Secure Shell (SSH). SSH es un protocolo para iniciar sesiones en máquinas remotas que ofrecen autenticación, confidencialidad e integridad**. SSH es una herramienta que permite realizar conexiones seguras entre equipos unidos mediante una red insegura, como puede ser Internet**. **Utiliza el puerto 22 y sigue el modelo cliente-servidor**. La seguridad de Ssh se basa en la utilización de mecanismo de criptografía, de forma que toda transmisión de información es cifrada y el mecanismo de autenticación es transparente al usuario.

Ventajas de utilizar SSH:

- Después de la primera conexión, el cliente puede saber que se está conectando al mismo servidor en futuras sesiones.
- El cliente transmite al servidor la información necesaria para su autenticación en formato cifrado .
- Todos los datos que se envían y se reciben durante la conexión son cifrados.
- El cliente puede ejecutar aplicaciones gráficas desde el Shell.
- Integridad, confidencialidad y seguridad de datos.
- Las VPN reducen los costos y son sencillas de usar.
- Facilita la comunicación entre dos usuarios en lugares distantes.